INFORMATION SECURITY POLICY

I. POLICY

The Centers for Disease Control (CDC)* policy is that personnel take necessary and appropriate actions to protect information from disclosure or other inappropriate release in accordance with its level of classification.

II. PURPOSE

The purpose of this policy issuance is to establish responsibilities and provide guidance for the logging, control, transmission, and accountability of classified material and sensitive data documents.

Information protected under confidentiality and privacy laws and regulations are covered under other CDC policies.

III. DEFINITIONS

"Document security" is the safeguarding of classified information, the unauthorized disclosure of which could harm, tend to impair, or otherwise adversely affect the national defense.

"Classified defense material," "classified information," "classifiedmaterial," and all other terms where the word "classified" is used mean official information requiring protection in the interest of national defense.

III. DEFINITIONS (Continued)

"Administratively controlled" means to protect certain types of privileged information which are not entitled to protection or

classification.

"Physical security" is the safeguarding of CDC property and materials.

"Personnel security" is the background investigation and clearance of employees for authorizing access to classified information and material.

IV. SCOPE

This policy applies to all classified information and material (electronic or other) transmitted to or from, stored, logged, or otherwise controlled by CDC.

V. GUIDANCE

The HHS Information Security Manual, E.O. 12356, and other National Security Agency directives provide additional guidance in this area.

VI. RESPONSIBILITIES

Responsibility for Federal civilian secure communications activities is assigned to the National Security Agency, Civilian Liaison.

The Division of ADP and Telecommunications Resources, Office of the Secretary, HHS is the focal point for all security activities of the Department.

The Director, Office of Program Support, has been designated as the CDC Security Representative.

The Information Resources Management Office (IRMO) has primary responsibility for information security at CDC. The IRMO is responsible for the operation of the Secure Communications Facilities of CDC and IRMO staff have been appointed as CDC Logging Control Officer and COMSEC Custodian.

The Office of Program Support has primary responsibility for physical security at CDC.

The Personnel Management Office has primary responsibility for personnel security at CDC.

The Center for Environmental Health and Injury Control, Center for Prevention Services, Agency for Toxic Substances and Disease Registry, and International Health Program Office have designated custodians for

safes where classified information may be stored.

Responsibility for the protection of classified information and material in the custody of CDC rests with each individual having such information or knowledge no matter how it was obtained. Each individual will be directly responsible for adhering to all regulations which are issued for protection of classified information.

Any employee having knowledge of the loss or possible subjection to compromise of any classified information or material should promptly report the circumstances to the appropriate security representative.

VII. SECURITY DESIGNATIONS

A. Top Secret

This designation will be applied only to information or material when the unauthorized disclosure of such could reasonably be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include armed hostilities against the United States or its allies, disruption of foreign relations vitally affecting the national security, the compromise of vital national defense plans or complex cryptologic and communications intelligence systems, the revelation of sensitive intelligence operations, and the disclosure of scientific or technological developments vital to national security.

B. Secret

This designation will be applied only to information or material when the unauthorized disclosure of such could reasonably be expected to cause serious damage to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security, significant impairment of a program or policy directly related to the national security, revelation of significant military plans or intelligence operations, compromise of significant military plans or intelligence operations, and compromise of significant scientific or technological developments relating to national security.

C. Confidential

This designation will be applied only to information or material when the unauthorized disclosure of such could reasonably be expected to cause damage to the national security. Examples of damage include the compromise of information that indicates strength of ground, air, and naval forces in the United States and overseas areas; disclosure of

technical information used for training, maintenance, and inspection of classified munitions of war; revelation of performance characteristics, test data, design, and production data on munitions of war.

D. Limited Official Use and Official Use Only

These designations will be applied to material which is not entitled to protection or classification under Executive Order 12356 but which is privileged for other than defense reasons. Material marked LIMITED OFFICIAL USE requires the same protection as CONFIDENTIAL defense information.

E. Restricted Data

This is an additional category of defense information, defined by the Department of Energy as data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power. It is distinguishable from other classified material by the following marking which appears on the first page of the document (and the front cover, if there is one):

RESTRICTED DATA

This document contains restricted data as defined in the Atomic Energy Act of 1946. Its transmittal or the disclosure of its contents in any manner to an unauthorized person is prohibited.

RESTRICTED DATA also carries the marking TOP SECRET, SECRET, or CONFIDENTIAL, as warranted by the security importance of the material.

VIII. PROCEDURES

A. Authority

In the Department of Health and Human Services only the Secretary may exercise classification authority. This authority cannot be delegated by the Secretary to any other employee of the Department.

B. Custody and Safekeeping

Classified information will be stored only under conditions adequate to prevent unauthorized persons from gaining access. The requirements specified in HHS Security Manual, Chapter 3, will be observed at all

times.

Upon direct receipt of classified material, the individual will immediately deliver it to the Logging Control Officer for logging and preparation for processing.

Classified material should not be delivered to or left exposed in unoccupied offices. Under no circumstances should classified material be stored or placed in desk drawers. Employees using classified material will take every precaution to prevent deliberate or casual inspection of it by unauthorized persons. All copies and informal material such as memorandums, notes, drafts, carbon copies, and carbon paper will be safeguarded by the rules prescribed for other classified material.

No classified material should be allowed to remain outside the official security safe(s) overnight nor will it be allowed to be taken home or carried onboard an aircraft or similar transportation. Material checked out during the day must be returned to the Logging Control Officer or appropriate CIO custodians by 5 p.m. the same day.

C. Dissemination

No employee should release classified information to another person without first determining whether that person is cleared to receive such information and have a need to know. Security clearance information may be obtained from or through the CDC Personnel Security Representative.

CLASSIFIED INFORMATION WILL BE ENTRUSTED ONLY TO INDIVIDUALS WHOSE OFFICIAL DUTIES REQUIRE KNOWLEDGE OR POSSESSION OF SUCH INFORMATION. AN EMPLOYEE IS NOT AUTHORIZED TO GAIN POSSESSION OF CLASSIFIED INFORMATION MERELY BY VIRTUE OF HIS OR HER GRADE OR POSITION.

Public or private discussion of classified information with or in the presence or hearing of any person not authorized to have knowledge thereof is strictly forbidden.

Before any employee may have access to RESTRICTED DATA, he or she must have a special (Class "Q") clearance issued by the Department of Energy. Control and dissemination of RESTRICTED DATA will be made in accordance with the regulations of the Department of Energy.

Officials and employees of CDC should not discuss or make available to foreign nationals or foreign governments any classified defense information.

It is permissible to make reference by unsecure telephones to nontelegraphic classified material if such references do not reveal the substance of the material under discussion. References to file numbers, dates, and subjects (provided the subject itself is not classified) may be made over an unclassified telephone if care is exercised not to reveal the substantive material.

Classified and administratively controlled telegrams or documents may be read only on the Secure Voice Units located at the Clifton Road and Chamblee facilities. The CDC has the capability to talk at the TOP SECRET level on the Secure Voice Units. Individuals who desire to originate a call on the Secure Voice Unit must be verified by either the Logging Control Officer or Personnel Security Representative that they have appropriate security clearance.

D. Conferences and Meetings

Conferences or meetings to discuss classified information should be scheduled in the Secure Conference Room. Every precaution will be observed to ensure that the participants are entitled to receive such information on a need-to-know basis, and that all participants possess suitable security clearances. To arrange meetings in the Secure Conference Room, call the Communications Center on extension 3030.

Before the meeting is adjourned, agreement will be reached on the proper classification of the minutes, if such were kept, and the participants again reminded of the proper safeguarding of such classified information as they received during the course of the meeting.

---

*References to CDC also apply to the Agency for Toxic Substances and Disease Registry.